HEALTH INFORMATION SECURITY AND PRIVACY COLLABORATION (HISPC) PROJECT

Proposed Process for Deliverable One: Variations Report

1. Create documents that categorize and identify information for each scenario by:
    a. Domain
    b. Stakeholder
    c. Wisconsin law/HIPAA
2. Consumer Interests Workgroup review documents
3. Design process for convening stakeholder groups (including developing the necessary tools, e.g., framework or worksheet for analyzing policies and practices by scenario)
4. Consumer Interests Workgroup review process
5. Data gathering (convening stakeholder groups)
6. Analyze and record results
7. Consumer Interests Workgroup review of the results/products/reports

(See next page for key project terms)

Key Project Terms

Scenario

The grantor worked with the American Health Information Management Association (AHIMA) to develop 18 scenarios in which health information is accessed or exchanged. Stakeholders will be asked to share organizational policies and practices for each scenario, providing a snapshot of commonalities and variations in policy and practice in Wisconsin and identifying possible barriers to health information exchange.

Domain

HISPC examines privacy and security in nine domains:

- User and entity authentication used to verify that a person or entity seeking access to electronic personal information is who they claim to be.
- Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.
- Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.
- Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.
- Information protections so that electronic personal health information cannot be improperly modified.
- Information audits that record and monitor the activity of health information systems.
- Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.
- State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.
- Information use and disclosure policies that arise as health care entities share clinical health information electronically.

Stakeholder

HISPC identifies a number of stakeholder groups to weigh in on appropriate scenarios, including:

- Clinicians
- Physician groups
- Federal health facilities
- Hospitals
- Payers
- Public health agencies
- Pharmacies
- Laboratories
- Health centers
- Homecare and hospice
- Correctional facilities
- Professional associations and societies
- Medical and public health schools that undertake research
- Quality improvement organizations
- Consumers or consumer organizations
- State government
- Long term care facilities and nursing homes
- Community clinics and health centers